MANUAL DE CARGOS

Dependencia:	División Operaciones de Servicios	**Área:**	Área de Cómputo
Código del Cargo:	3011.XX	**Código del Puesto:**	3011
Categoría	21	**Nombre del Puesto:**	Profesional PED 2
Nombre del Cargo:	Gestor de Respaldos	**Reporta a:**	Jefe Área de Cómputo
Objetivo del Cargo:	Establecer, administrar y controlar el proceso de respaldos, plan integral de respaldos y recuperación de toda la información a nivel conglomeral, mediante las normas y políticas definidas por la administración de datos, mismas que deben estar alineadas con los objetivos y estrategias del Conglomerado Financiero Banco Popular. Es responsable de gestionar la ejecución y restauración de los respaldos efectuados en la Dirección de Tecnología de Información.		

MACRO PROCESO	PROCESO	ACTIVIDAD		FUNCIONES PRINCIPALES
			1	Planear y organizar el trabajo en coordinación con su superior inmediato.
			2	Permanecer actualizado en cuanto a los cambios, nuevas tendencias y buenas prácticas que se susciten en el ámbito de los respaldos.
			3	Acatar y velar por el cumplimiento de normas, leyes, procedimientos y políticas, tanto internas como externas que involucren el tema de respaldos.
			4	Evacuar consultas y atender solicitudes de clientes internos, así como participar en diferentes actividades cuando sea solicitado por la jefatura.
			5	Brindar apoyo, asesoría y capacitación a las distintas área del Banco que lo requieran, de acuerdo con las actividades desempeñadas.
			6	Velar porque los trabajos encomendados se cumplan oportunamente y de acuerdo con las fechas establecidas.
			7	Participar en proyectos informáticos cuando le sea solicitado.
			8	Cumplir con los estándares de calidad en la ejecución de sus labores.
			9	Ejecutar otras tareas propias del puesto.
				FUNCIONES ESPECÍFICAS
			10	Definir y planificar las necesidades de respaldo requeridas por los dueños de las aplicaciones.
			11	Consolidar las necesidades de respaldo, almacenamiento, conservación, seguridad, recuperación y desecho de los datos.
			12	Establecer modelos, arquitectura y planes integrales de respaldos en alineamiento con los requisitos de negocio, planes de continuidad de TI y seguridad de la información.
			13	Definir los requisitos de almacenamiento de respaldos en concordancia en la planificación del ciclo de vida de la información, detallando los niveles de almacenamiento y capacidades requeridas en cada nivel.
			14	Investigar, evaluar y proponer posibles soluciones para los respaldos de la información.
			15	Establecer los requerimientos para crear, emitir, actualizar y comunicar directrices, políticas, normas y procedimientos u otra documentación relacionada con los respaldos de información, mismo que deben estar alineados con los objetivos o estrategias de negocio definidos por el Banco.
			16	Actualizar los acuerdos de respaldos y restauración según los requerimientos del negocio.
			17	Controlar que las normas y políticas establecidas para la administración de datos se cumplan fielmente, estableciendo los controles necesarios y ejecutando los procedimientos operativos que correspondan.
			18	Establecer las directrices para la gestión de respaldos y la restauración de sistemas de información, configuraciones de equipos e información, contenidas en los sistemas de información.
			19	Definir, proponer e implementar métricas de evaluación de la eficacia de los respaldos de la información efectuados en las diferentes plataformas tecnológicas.
			20	Establecer un esquema referente a los respaldos de información de los usuarios finales y controlar que se cumplan según lo establecido.
			21	Delimitar las políticas referentes a los respaldos de información de los usuarios finales y controlar que se cumplan según lo establecido.
			22	Controlar que los procesos de verificación del contenido de los respaldos, cumplan con lo establecido en la metodología de respaldos de tecnología de información, según los lineamientos del proceso de Administración de Datos (DS11), COBIT.
			23	Verificar que los procesos ejecutados para realizar los respaldos y pruebas de reanudación se efectúen de forma correcta, en caso contrario investigar las causas y proponer soluciones efectivas.
			24	Realizar los informes sobre respaldos correspondientes a; incidentes presentados, resueltos, estadísticas y todos aquellos requeridos, según operativa de respaldos.
			25	Realizar procedimientos operativos informáticos, rutinarios o especiales, calendarizados o no, que requieren la verificación de la información respaldada en medios magnéticos, para asegurar las recuperaciones de datos y/o continuidad de los servicios del Banco.
			26	Atender y gestionar la solución a los requerimientos informáticos que le sean asignados relacionados con los respaldos de información, calendarización de procesos, investigaciones y procesos especiales; así como consultas de las distintas áreas del Banco.
			27	Participar en la evaluación de los procedimientos y manuales operativos informáticos para la aprobación de la puesta en producción de nuevos sistemas o procesos en el ámbito de respaldos.
			28	Participar en las evaluaciones del riesgo operativo, en el tema de respaldos, implícitos en los manuales y procedimientos operativos informáticos y hacer las recomendaciones para minimizar el riesgo.
			29	Identificar y registrar los nuevos procesos que generan respaldos de información o datos, procesos eventuales no calendarizados y realizar las acciones requeridas para elaborar las órdenes de trabajo con las instrucciones y pasos a seguir, de manera que se asegure la información por alguna situación de contingencia.
			30	Validar que los incidentes presentados producto de los respaldos, se les proporcione una solución en el tiempo definido y en caso de no resolverse en plazo establecido, proponer las acciones respectivas.
			31	Velar porque las pruebas de restauración se realicen en el periodo establecido, en las políticas de respaldo de la información.
			32	Participar en conjunto con las dependencias respectivas en temas concernientes a respaldos de información, planes de recuperación ante desastres y toda aquellas actividades que minimicen los problemas para la reanudación de la información y aseguren el levantamiento de los equipos.
			33	Administrar el inventario de medios magnéticos con respaldo de información o datos que se almacenan en los diferentes sitios; además, de velar porque el inventario se efectúe según los lineamientos de los equipos.
			34	Asegurar que los procesos de reutilización, eliminación y desecho de medios de almacenamiento de información, se realicen en forma apropiada, basada en las normas de seguridad informática establecidas y según COBIT.
				FUNCIONES RELACIONADAS CON RIESGO
			35	Realizar una adecuada gestión de los riesgos, identificando, valorando y controlando aquellos que puedan impactar los Planes Estratégicos del Conglomerado a los cuales se encuentran asociados.
			36	Identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, relacionados directamente a la administración de los riesgos operativos, normativos, financieros, de proyectos, tecnológicos y reputacionales, según corresponda.
			37	Ejecutar los lineamientos establecidos en la metodología institucional de administración de riesgos del Conglomerado Financiero, así como las herramientas y técnicas para identificar los distintos tipos de riesgos a que se encuentra expuesta la entidad.
			38	Desarrollar las actividades relacionadas con la atención de los Planes de Mitigación de los riesgos identificados dentro de los procesos de la dependencia asignada.
			39	Dar seguimiento al control y fiscalización a las medidas adoptas para el funcionamiento del sistema de valoración del riesgo, garantizando una adecuada cultura de riesgo.
			40	Asegurar que el personal a su cargo conozca sobre la normativa de riesgo aplicable a su área, como parte de la Cultura de Riesgo.
			41	Le puede corresponder participar activamente en los diferentes Comités o comisiones definidos para el Conglomerado para conocer los planes de acción y medidas a tomar para minimizar el impacto de los riesgos inherentes en su campo de acción.
			42	En caso de materializarse un evento de riesgo es responsable de reportarlo directamente a la Dirección Corporativa de Riesgo, para su análisis y seguimiento.
			43	Vigilar que el traslado de los medios magnéticos a los sitios alternos y contingente, se ejecuten bajo las normas de seguridad de información dictadas.
				FUNCIONES RELACIONADAS CON SUGEF
			44	Según el Acuerdo SUGEF 14-17 "Reglamento General de Gestión de la Tecnología de Información", el cual establece los requerimientos mínimos para la gestión de tecnología de información que deben de acatar las entidades supervisadas y reguladas del sistema financiero costarricense y en concordancia con la Ley de Control Interno, Capítulo III, Sección I "Deberes del jerarca y los titulares subordinados", capítulo 12,13 y 14, este puesto es responsable del desarrollo de las actividades y tareas que le asignen velando por un adecuado ejercicio del mismo, debe garantizar la eficiencia y eficacia de las operaciones que le corresponde ejecutar tomando las medidas correctivas en beneficio de la institución. Por el nivel del puesto deberá promover mecanismos y procesos que mejoren el sistema de control interno en la gestión que le corresponde realizar. Debe procurar mantener las operaciones con un nivel de riesgo aceptable.

CODIGO		REQUISITOS EXIGIBLES
	Formación Académica:	Licenciatura en Ingeniería de Sistemas u otra carrera afín relacionada con las funciones del puesto.
	Legales:	Incorporación al Colegio de Profesionales respectivo.
	Experiencia:	Tres años de experiencia en labores propias a las descritas.

CODIGO	* REQUISITOS TÉCNICOS EXIGIBLES
	1. Certificados de participación en los siguientes cursos: Análisis de Impacto de Negocio-BIA basado en la Norma ISO-22317 Clasificación de información Sensible y Crítica Gestión de Continuidad Tecnológica basada en Mejores Prácticas

*** Los requisitos técnicos exigibles deben ser presentados con respaldo por medio de certificaciones de participación, aprovechamiento, cursos o similares. Los requisitos técnicos exigibles serán evaluados por medio de la prueba de conocimiento que forma parte del proceso de selección.**

CODIGO	REQUISITOS TÉCNICOS DESEABLES
	1. Certificados de participación en los siguientes cursos: Implementación de Continuidad de Negocios en Mejores Prácticas y Alineamiento con ISO-22301 Fundamentos de Cobit Manejo Estratégico de Crisis en las organizaciones BIG DATA y Ciencia de los Datos-Introducción
	2. Conocimientos en administración y configuración de Herramientas de Back up, gestión de Políticas de Back up & Restore definición de Schedules y Políticas de Retención (se valorará especialmente conocimiento de la solución AVAMAR/DATADOMAIN).
	3. Conocimientos de Networker, EMC DPA

CODIGO	SISTEMAS UTILIZADOS

COMPETENCIAS REQUERIDAS

PERFIL KOMPE DISC:		PERFIL: PROFESIONALES SOPORTE			
CODIGO	**Cardinales**	**D**	**C**	**B**	**A**
CAR-01	Compromiso Social				
CAR-02	Orientación al Cliente				
CAR-03	Innovación y Creatividad				
CAR-04	Orientación al Logro				
CAR-05	Seguimiento de procedimientos				
CODIGO	**Gerenciales**	**D**	**C**	**B**	**A**
GER-01	Desarrollo de Otros				
GER-02	Dirección de Equipo				
GER-03	Seguimiento de la Gestión				
CODIGO	**Negocio**	**D**	**C**	**B**	**A**
NEG-01	Análisis de la Información				
NEG-02	Negociación				
NEG-03	Persuasión				
NEG-04	Manejo Emocional				
NEG-05	Trabajo en Equipo				
CODIGO	**Soporte**	**D**	**C**	**B**	**A**
SOP-01	Planeación				
SOP-02	Practicidad				
SOP-03	Precisión				
CODIGO	**DISC - Personalidad**	**D**	**C**	**B**	**A**
DISC-01	Dominancia				
DISC-02	Influencia				
DISC-03	Estabilidad				
DISC-04	Conformidad				

Observaciones:	**Se aprueba el perfil en oficio GGC-0561-2018 (23-05-2018) por estudio de División Gestión de Calidad "Estudio Técnico de Análisis de Actividades Relacionadas con la Iniciativa 14 Respaldos de Información".** **Se incluyen Funciones de Riesgo las cuales se incorporan a los perfiles con la aprobación de la Gerencia General Corporativa, emitida en el HT-493-GGC-2019, de fecha el 14 de octubre 2019. Referencia: DIRGE-689-2019 / DIRCH-1477-2019.**